COVER PAGE

Hewlett-Packard Docket Number:

200314073-1

Title:

COMPUTER SECURITY SYSTEM AND METHOD

Inventors

Matthew J. Wagner
14123 Armant Place Drive
Cypress, Texas 77429
USA

Valiuddin Ali
6830 Champions Plaza Drive, #1004
Houston, Texas 77069
USA

Manuel Novoa
16226 Morning Pine Trail
Cypress, Texas 77433
USA

COMPUTER SECURITY SYSTEM AND METHOD

TECHNICAL FIELD

[0001] The present invention relates generally to the field of computer systems and, more particularly, to a computer security system and method.

BACKGROUND

[0002] Some computer systems, computer peripheral devices, and other types of computer resource devices comprise a self-managed authentication mechanism such that a security credential provided by a user to access the resource device is verified or authenticated by the resource device without relying on an external authentication service or entity. However, many users are either unaware that such an authentication system exists on the resource device or, if used, a generally "weak" security credential is provided by the user, thereby rendering the resource device susceptible to attack (i.e., a shorter, more familiar and, therefore, more easily compromised password). Security credentials having a more complex or longer character string, resulting in a stronger security credential, are increasingly difficult for the user to remember or to input.

SUMMARY

[0003] In accordance with one embodiment of the present invention, a computer security system comprises a self-managed device having an authentication system for controlling access to the self-managed device by a user. The system also comprises a security module adapted to authenticate an identity of the user and, in response to user authentication, automatically generate, transparently to the user, device credential data verifiable by the authentication system to enable user access to the self-managed device.

[0004] In accordance with another embodiment of the present invention, a computer security method comprises authenticating an identity of a user and automatically generating transparently to the user, in response to user authentication, device credential data verifiable by an authentication system of a self-managed device to enable user access to the self-managed device.

[0005] In accordance with yet another embodiment of the present invention, a computer security system comprises a security module executable by a processor and adapted to access credential data to verify an identity of a user. The system also comprises an activation/deactivation module accessible via a networked administration client. The activation/deactivation module is adapted to interface with the security module in response to a request by the administration client to activate, transparently to the user, an authentication system of a self-managed device to control user access to the self-managed device.

BRIEF DESCRIPTION OF THE DRAWINGS

[0006] For a more complete understanding of the present invention and the advantages thereof, reference is now made to the following descriptions taken in connection with the accompanying drawings in which:

[0007] FIGURE 1 is a diagram illustrating an embodiment of a computer security system in accordance with the present invention;

[0008] FIGURE 2 is a flow chart illustrating an embodiment of a computer security method in accordance with the present invention;

[0009] FIGURE 3 is a flow chart illustrating another embodiment of a computer security method in accordance with the present invention; and

[0010] FIGURE 4 is a flow chart illustrating yet another embodiment of a computer security method in accordance with the present invention.

DETAILED DESCRIPTION OF THE DRAWINGS

[0011] The preferred embodiments of the present invention and the advantages thereof are best understood by referring to FIGURES 1-4 of the drawings, like numerals being used for like and corresponding parts of the various drawings.

[0012] FIGURE 1 is a diagram illustrating an embodiment of a computer security system 10 in accordance with the present invention. In the embodiment illustrated in FIGURE 1, system 10 comprises a user client 12 coupled to an administration client 14 via a communications network 16. Communications network 16 may comprise any type of wired or wireless network now known or later developed. Briefly, system 10 provides for

automatic activation and/or deactivation of an authentication system for a self-managed device such as, but not limited to, a hard drive, peripheral device, or other type of computer resource, by an administrator via administration client 14 or by a user of client 12. As used herein, a "self-managed device" comprises any type of computer resource or device adapted to authenticate security credentials for a user to access or initiate operations on the resource or device independent of an external computer resource. It should be understood that more than one self-managed device may reside on or form a part of a particular computer resource (e.g., a basic input/output system (BIOS) and hard drive of a desktop computer), a particular computer resource may itself comprise a self-managed device (e.g., a server), and a particular self-managed device may itself comprise a plurality of computer resources. In operation, system 10 automatically generates, transparently to the user, a security credential to be used by a corresponding self-managed device for access authentication. The security credential is transmitted, transparently to the user, to the self-managed device and stored by the self-managed device. Thus, for subsequent access requests to the self-managed device by a user, after verification of the identity of the user, a security credential is automatically transmitted to and authenticated by the self-managed device transparently to the user.

[0013] In the embodiment illustrated in FIGURE 1, client 12 comprises a processor 20, a network interface 22, and an input/output (I/O) controller 24. Network interface 22 enables communications between user client 12 and administration client 14 via communication network 16. In FIGURE 1, a single user client 12 is illustrated; however, it should be understood that additional user clients 12 may also be networked for system 10. I/O controller 24 enables control of various types of input device(s) 30 and output device(s) 32 for receiving information from a user of client 12 and outputting information to a user of client 12, respectively. Input device(s) 30 may comprise a keyboard, mouse, trackpad, modem, microphone, or any other type of device for inputting information to client 12. Output device(s) 32 may comprise a display monitor, speakers, a printer, or any other type of device for outputting information from client 12.

[0014] As illustrated in FIGURE 1, system 10 also comprises a basic input/output system (BIOS) 40 stored in a memory 42 for performing booting or starting operations such as system initialization and tests and peripheral component registration operations. For example, upon booting or starting of client 12, processor 20 passes control to BIOS 40 to identify and ascertain the hardware and software resources connected to, or forming a part of,

client 12. BIOS 40 also generally verifies that the connected hardware components are working properly and loads all or a portion of an operating system. All or a portion of BIOS 40 may be stored in various types of memory 42. For example, all or a portion of memory 42 may comprise read-only memory (ROM), erasable programmable read-only memory (EPROM), volatile or flash ROM, or other types of memory now known or later developed.

[0015] In the embodiment illustrated in FIGURE 1, BIOS 40 also comprises a security module 44. Security module 44 may comprise hardware, software, or a combination of hardware and software. Briefly, security module 44 is used to verify or authenticate the identity of a user of client 12 and automatically activate and/or deactivate an authentication system of a self-managed device. Additionally, security module 44, transparently to the user, automatically generates and/or transmits a security credential to a corresponding self-managed device so that the corresponding self-managed device may use the generated and received security credential to verify subsequent access to the device by the user transparently to the user. In FIGURE 1, security module 44 is illustrated as a component of BIOS 40; however, it should be understood that security module 44 may be otherwise stored, located and/or accessible on client 12 to accommodate a variety of self-managed device security applications.

[0016] In the embodiment illustrated in FIGURE 1, security module 44 comprises a registration module 50 and a credential controller 52. Registration module 50 is used to identify self-managed devices coupled to client 12 or configured as a component of client 12 such that security module 44 may be used to activate and/or deactivate an authentication system of a particular self-managed device. For example, in operation, registration module 50 may perform a registration operation to identify and register each available self-managed device coupled to client 12 or configured as a component of client 12. The information obtained by registration module 50 may be stored in memory 42 as device data 70.

[0017] Credential controller 52 is used to verify or authenticate a security credential corresponding to a user of client 12 and/or automatically generate or transmit a security credential to a corresponding self-managed device for subsequent authentication operations performed by the self-managed device. For example, in the embodiment illustrated in FIGURE 1, credential controller 52 comprises a credential verifier 60 and a credential generator 62. Credential verifier 60 is used to verify or authenticate an identity or other type of security information corresponding to a user of client 12. For example, as

illustrated in FIGURE 1, user data 72, security credential data 74, and relational data 76 are stored in memory 42 so as to be accessible by security module 44. User data 72 comprises information associated with each user of client 12 such as, but not limited to, the identity of the user, an Internet protocol (IP) address associated with client 12, or other type of information associated with either a user of client 12 or information associated with client 12. Thus, for example, user data 72 may comprise an alphanumeric character string indicating a username or other type of user identification information that a user inputs to client 12 and that is verifiable by credential verifier 60 based on user data 72.

[0018] Security credential data 74 comprises security information associated with accessing or initiating operations on a secure computer resource. For example, in the embodiment illustrated in FIGURE 1, security credential data 74 comprises access credential data 80 and device credential data 82. Access credential data 80 comprises information associated with verifying or authenticating an identity of a user for accessing or initiating operations on a particular computer resource such as, but not limited to, client 12. For example, access credential 80 may be used by verifier 60 in association with user data 72 to verify the identity of a user. Thus, for example, to access or initiate operations on client 12, verifier 60 may access user data 72 and access credential data 80 to verify or authenticate a username and password input by the user to access client 12. In some embodiments, client 12 may also be configured for pre-boot authentication such that an access security credential 80, such as a password or other type of security credential, is provided by a user of client 12 for initiating a booting operation of client 12.

[0019] Device credential data 82 comprises information associated with security credentials for accessing or initiating operations of a self-managed device. For example, device credential data 82 comprises information used by a self-managed device to verify or authenticate access to a secure self-managed device. Relational data 76 comprises information associated with relating user data 72 to security credential data 74. For example, for each user of client 12, various types of security credentials may be stored in memory 42 corresponding to accessing or initiating operations on client 12 or accessing or initiating operations of self-managed device(s). Relational data 76 correlates access credential data 80 and/or device credential data 82 to user data 72. However, it should also be understood that information correlating or otherwise relating a particular user to credential data 74 associated with the particular user and/or device(s) 90 controlled via security module 44 for the

particular user may be otherwise performed (e.g., populating fields of user data 72 with information identifying device(s) 90 secured via module 44 for the user and/or credential data 82 for each device secured using module 44 for the particular user).

[0020] Credential generator 62 automatically generates a security credential for authentication use by a corresponding self-managed device and/or transmits the generated security credential to the corresponding self-managed device transparently to the user. For example, in operation, credential verifier 60 receives an access credential data 80 from a user of client 12 and verifies or authenticates the access credential data 80 based on user data 72. During an initial enablement operation for an authentication system of a particular self-managed device, credential generator 62 automatically generates device credential data 82 for the corresponding self-managed device. For example, in some embodiments, credential generator 62 may randomly generate an alphanumeric character string or other type of security credential that will be used by the corresponding self-managed device for authentication operations. In some embodiments, credential generator 62 may generate the corresponding self-managed device security credential based on user data 72 and/or access credential data 80. For example, credential generator 62 may generate the corresponding self-managed device security credential by hashing user data 72 with access credential data 80. The security credential generated by credential generator 62 is stored in memory 42 as device credential data 82. Additionally, credential controller 52 correlates device credential data 82 generated by credential generator 62 with user data 72.

[0021] In the embodiment illustrated in FIGURE 1, a self-managed device 90 resides on client 12. For example, in the illustrated embodiment, self-managed device 90 comprises a hard drive 100 having a processor 102 and a memory 104. As described briefly above, self-managed device 90 is configured to verify or authenticate a security credential without relying on an external authentication mechanism. For example, in the embodiment illustrated in FIGURE 1, device 90 comprises an authentication system 110. Authentication system 110 may comprise hardware, software, or a combination of hardware and software. In the embodiment illustrated in FIGURE 1, authentication system 110 comprises a credential validator 120. Briefly, credential validator 120 verifies or authenticates device credential data 82 received from security module 44 to authorize access or initiate operations of hard drive 100. Information associated with verifying or authenticating device credential data 82 may be stored as credential data 130 in memory 104.

[0022] In the embodiment illustrated in FIGURE 1, client 12 also comprises an activation/deactivation module 140 stored in a memory 142. Activation/deactivation module 140 may comprise hardware, software, or a combination of hardware and software. Briefly, activation/deactivation module 140 is executable by processor 20 to provide an interface for a user of client 12 to activate and/or deactivate an authentication system of a particular self-managed device coupled to or forming a part of client 12. For example, in operation, a user of client 12 may desire to activate and/or deactivate an authentication system associated with a particular self-managed device. Activation/deactivation module 140 provides an interface to security module 44 such that the user of client 12 may select a desired self-managed device for authentication system activation or deactivation from a listing of registered self-managed devices presented or displayed to the user. In response to a selection by a user of a particular self-managed device, activation/deactivation module 140 automatically interfaces with security module 44 to initiates the corresponding activation or deactivation operation for the authentication system of the selected self-managed device.

[0023] Thus, in operation, during a booting or other operation of client 12, security module 44 may request and receive from a user of client 12 user data 72 and/or access credential data 80 to control access to client 12 and/or initiate a booting or other operation of client 12. Security module 44 may also perform a registration operation using registration module 50 to identify each self-managed device available for authentication system activation or deactivation.

[0024] To activate or deactivate an authentication system of a particular self-managed device, the user of client 12 may initiate or activate activation/deactivation module 140. Activation/deactivation module 140 interfaces with security module 44 to provide a listing or display of registered self-managed devices for authentication system activation or deactivation. Activation/deactivation module 140 receives a selection of a particular self-managed device for authentication system activation or deactivation and interfaces with security module 44 to perform the desired activation or deactivation operation. In some embodiments, security module 44 may also be configured to automatically activate and/or deactivate all or a portion of the registered self-managed devices during a booting or other operation, thereby enabling automatic authentication system control and policies to be implemented on any client 12.

[0025] To activate an authentication system for a particular self-managed device, credential controller 52 accesses user data 72 and/or access credential data 80 to verify or authenticate an identity of a particular user of client 12 using credential verifier 60. After user authentication, credential generator 62 automatically generates device credential data 82 for a desired self-managed device. For example, credential generator 62 may randomly generate a password or other type of security credential at a predetermined level of complexity or strength and transmit the generated device credential data 82 to a particular self-managed device such as, for example, self-managed device 90. Self-managed device 90 stores the device credential data 82 as credential data 130 in memory 104. Credential validator 120 uses the credential data 130 to verify or authenticate access to device 90 for subsequent operations. Credential controller 52 also correlates the generated device credential data 82 for each use of client 12 via relational data 76.

[0026] In some embodiments, client 12 may be configured to automatically authorize access to all or a portion of the registered self-managed devices during a booting or other operation of client 12 or may be configured to authorize access to particular self-managed devices as the user desires access to the particular self-managed device. For example, security module 44 may be configured to automatically transmit device credential data 82 to each corresponding self-managed device upon verification of user data 72 and/or access credential data 80. Thus, during a booting or other operation of client 12, security module 44, transparently to the user of client 12, transmits device credential data 82 to all or a portion of the registered self-managed devices such that the authentication system of each corresponding self-managed device may verify or authenticate the device credential data 82 for accessing or initiating operations using the corresponding self-managed device. Alternatively or additionally, security module 44 may be configured to transmit device credential data 82 to a particular self-managed device 90 in response to a request by a user of client 12 to access or initiate operations for a particular self-managed device 90. Thus, in this application, in response to a request or operational function initiated by a user of client 12, security module 44, transparently to the user, transmits device credential data 82 to a corresponding self-managed device for authentication by the self-managed device.

[0027] In the embodiment illustrated in FIGURE 1, administration client 14 comprises a processor 150, a network interface 162, and a memory 154. Network interface 152 enables communications between administration client 14 and user client 12 via

communication network 16. As illustrated in FIGURE 1, administration client 14 also comprises a security administration module 160. Security administration module 160 may comprise software, hardware, or a combination of software and hardware. In FIGURE 1, security administration module 160 is illustrated as being stored in memory 154 so as to be executable by processor 150. However, it should be understood that security administration module 160 may be otherwise stored, even remotely, so as to be accessible and executable by processor 150.

[0028] As illustrated in FIGURE 1, security administration module 160 comprises a client activation/deactivation module 162 for interfacing with security module 44 of a particular user client 12 to activate or deactivate an authentication system 110 of a particular self-managed device 90. For example, administration client 14 comprises client data 166 stored in memory 154 having information associated with client 12 such as, but not limited to, available or registered self-managed devices 90 of client 12 having authentication systems 110 for activation or deactivation. Client data 166 may also comprise information associated with user data 72 and/or access credential data 80 such that a user of administration client 14 may provide proper security credentials for authentication by security module 44. User data 72 and/or access credential data 80 may also comprise information associated with verifying or authenticating access for administration personnel.

[0029] Thus, in operation, a user of administration client 14 may initiate client activation/deactivation module 162 to communicate with a particular client 12 via communication network 16 to activate or deactivate an authentication system 110 of a particular self-managed device 90. For example, in operation, client activation/deactivation module 162 may interface with security module 44 such that access credentials of administration client 14, or a user of administration client 14, may be verified by credential verifier 60. After security credential authentication, client activation/deactivation module 162 may be used to select a particular self-managed device 90 for authentication system 110 activation or deactivation. Based on a selection of a particular self-managed device 90 by a user of administration client 14, for authentication system 110 activation, security module 44 generates device credential data 82 via credential generator 62 and transmits the generated device credential data 82 to a corresponding self-managed device 90 such that device credential data 82 may be authenticated by authentication system 110 of the self-managed device 90 during subsequent operations. It should also be understood that system 10 may be

configured to enable automatic and transparent activation of an authentication system 110 of a device 90 from within an operating system (O/S) runtime environment.

[0030] Deactivation of an authentication system 110 for all or particular self-managed device(s) 90 may be accomplished in a manner similar as described above. For example, administration client 14 may interface with security module 44 of a particular client 12 via security administration module 160 to deactivate an authentication system 110 for all or particular self-managed device(s) 90 of client 12. A user of client 12 may also access or initiate activation/deactivation module 140 to deactivate an authentication system 110 for all or particular self-managed device(s) 90.

[0031] FIGURE 2 is a flowchart illustrating an embodiment of a computer security method in accordance with the present invention. The method begins at block 200, where registration module 50 of security module 44 performs a registration operation to identify and register self-managed device(s) 90 coupled to or configured as components of client 12. At block 202, client 12 initiates activation/deactivation module 140. For example, a user of client 12 may click on a desktop icon or perform some other function to launch or initiate activation/deactivation module 140. At block 204, activation/deactivation module 140 receives a request from a user of client 12 to activate an authentication system 110 for a particular self-managed device 90. At block 206, activation/deactivation module 140 receives a selection of a particular self-managed device 90 from the user. For example, as described above, activation/deactivation module 140 may present or display to the user a listing of registered self-managed devices 90 for authentication system 110 activation or deactivation.

[0032] At block 208, activation/deactivation module 140 interfaces with security module 44. At block 210, security module 44 verifies user data 72 received by a user of client 12 via credential verifier 60. At block 212, security module 44 verifies access credential data 80 received by a user of client 12 via credential verifier 60.

[0033] Upon verification of user data 72 and/or access credential data 80, credential generator 62 automatically generates device credential data 82, transparently to the user, for the desired self-managed device 90 at block 214. For example, as described above, credential generator 62 may randomly generate device credential data 82, transparently to the user, such that a generally complex or strong security credential may be used to control access to the desired self-managed device 90. At block 216, security module 44 transmits the

device credential data 82 to the corresponding self-managed device 90. At block 218, the device credential data 82 is stored in memory 104 of the corresponding self-managed device 90 as credential data 130 to enable the self-managed device 90 to authenticate access to the device 90 for subsequent access operations.

[0034] FIGURE 3 is a flowchart illustrating another embodiment of a computer security method in accordance with the present invention. The method begins at block 300, where client 12 receives a prompt or request from a user to access a secure self-managed device 90. At block 302, processor 20 initiates security module 44. At block 304, client 12 receives and/or verifies user data 72 associated with the user. At block 306, client 12 receives and/or verifies access credential data 80 associated with the user. For example, the user may input a username and password to client 12 to be verified by verifier 60 using user data 72 and/or access credential data 80 or, if a user is already logged into or performing operations on client 12, security module 44 may verify or authenticate previously received user data 72 and/or access credential data 80.

[0035] At decisional block 308, a determination is made whether user data 72 and/or access credential data 80 is verified for the particular user of client 12. For example, as described above, credential verifier 60 of security module 44 authenticates information received from a user of client 12 using user data 72 and/or access credential data 80. If the security credentials provided by the user of client 12 are not verified, the method returns to block 304. If the security information provided by the user is verified or authenticated by credential verifier 60, the method proceeds from block 308 to block 310, where security module 44 retrieves device credential data 82 for the corresponding self-managed device 90. Security module 44 may access relational data 76 to correlate device credential data 82 to a particular user and/or a particular self-managed device 90. At block 312, security module 44 automatically transmits device credential data 82 to the corresponding self-managed device 90 transparently to the user.

[0036] At block 314, device credential data 82 is received at the corresponding self-managed device 90. At the decisional block 316, a determination is made whether the received device credential data 82 is verified. For example, as described above, credential validator 120 may access credential data 130 and compare credential data 130 to the received device credential data 82. If the received credential data 82 is not verified, access to the self-managed device 90 is denied. If the received credential data 82 is verified or authenticated

by authentication system 110, the method proceeds to block 318, where authentication system 110 grants device 90 access.

[0037] Thus, security module 44 interfaces with a corresponding self-managed device 90, transparently to the user, to authenticate access to the device 90. It should also be understood that security module 44 and/or authentication system 110 may use a variety of encryption/decryption methods to generate and/or authenticate device credential data 82.

[0038] FIGURE 4 is a flowchart illustrating another embodiment of a computer security method in accordance with the present invention. The method begins at block 400, where processor 150 initiates security administration module 160. At block 402, network interface 152 accesses communications network 16. At block 404, security administration module 160 initiates communications with a desired client 12 via communications network 16.

[0039] At block 408, security module 44 of client 12 receives an activation or deactivation request from administration client 14 via client activation/deactivation module 162. At block 410, processor 20 initiates or activates security module 44 at client 12. At block 412, security module 44 identifies registered devices 90 available for activation or deactivation of a corresponding authentication system 110. For example, as described above, registration module 50 may be configured to display or provide a listing of registered devices 90 to administration client 14. At block 414, security module 44 receives a selection of a desired self-managed device 90 from administration module 14 via client activation/deactivation module 162. At block 416, security module 44 verifies user data 72 and/or access credential data 80 for the administration client 14 and/or user of administration client 14. At block 418, credential generator 62 automatically generates device credential data 82 for the desired self-managed device 90 transparently to the user. At block 420, security module 44 automatically transmits device credential data 82 to the corresponding self-managed device 90 transparently to the user. At block 422, the corresponding self-managed device 90 stores the device credential data 82 received from security module 44 as credential data 130 in memory 104. At block 424, security module 44 correlates device credential data 82 generated for a particular self-managed device 90 with corresponding user data 72 and/or access credential data 80.

[0040] Thus, embodiments of the present invention enable transparent generation and authentication of security credentials associated with self-managed devices 90, thereby

enabling "strong" security credentials (e.g., relatively long and complex credential(s)) to be used for controlling access to the device 90. Additionally, in the embodiment illustrated in FIGURE 1, security module 44 is illustrated as part of BIOS 40 such that portable devices 90 remain secure. For example, using a predetermined encryption/decryption technique, credential generator 62 may transmit encrypted device credential data 82 to device 90 such that credential validator 120 of device 90 decrypts the encrypted data 82 to authenticate access to device 90. However, it should be understood that security module 44 may also be otherwise stored on client 12 to enable a "logical" linking of security module 44 to portable devices 90 such that portable devices 90 remain secure.

[0041] Additionally, because device credential data 82 is generated and transmitted to device 90 transparently to the user, system 10 provides enhanced security for both online and offline applications. For example, for online applications, after user verification or authentication, relatively long and/or complex security credential(s) 82 are generated and transmitted to device(s) 90 transparently to the user, thereby eliminating or substantially reducing the likelihood that the security credential will be compromised by action of the user or by someone familiar with the user. In an offline application, if the self-managed device 90 is moved to another computer system, the self-managed device remains secure because security module 44 residing on the original computer system is "logically" linked to the self-managed device 90 because security module 44 transmits security credential 82 to the self-managed device 90 for authentication and verification. It should also be understood that system 10 may be configured to enable the user to detach or otherwise remove the "logical" binding between a particular self-managed device 90 and security module 44, thereby enabling use of the self-managed device 90 by another computer system.

[0042] It should be understood that in the methods described in FIGURES 2-4, certain functions may be omitted, combined, or accomplished in a sequence different than depicted in FIGURES 2-4. Also, it should be understood that the methods depicted in FIGURES 2-4 may be altered to encompass any of the other features or aspects described elsewhere in the specification.